NIHR | BioResource

NIHR BioResource

Information Governance (IG)

Policy

Version 4.2

06 May 2022

A. Document Purpose

(A): This document details the high-level Information Governance (IG) Principles that form the policy for all staff and partners of the National Institute for Health and Care Research (NIHR) BioResource for Translational Research (NIHR-BR). Information Governance at the NIHR BioResource is driven by information security protocols and research governance principles.

The NIHR-BR aims to meet the information governance and security requirements of industry recognised best practice and is committed to compliance with the NHS Digital Data Protection and Security Toolkit (https://www.dsptoolkit.nhs.uk/).

(B): The entity for these studies is NIHR BioResource for Translational Research, who are commissioned by NIHR and sponsored jointly by University of Cambridge and Cambridge University Hospitals NHS Foundation Trust.

(C): Cambridge University Hospitals NHS Foundation Trust (CUH) is the legal entity responsible for information governance.

(D): Scope - the Information Governance Policies apply to the information and operations supporting the collection of identifiable health-related and personal data for participants engaged in research studies, and to de-identified participant data.

(E): The NIHR-BR is a function which is managed within the confines of The University of Cambridge's operations. As such, the security and governance responsibilities for non-participant related research data and related activities (e.g. Finance and HR) build on those of the University. The BioResource's information governance and security policy framework therefore also builds upon the governance of policies and procedures of the University of Cambridge.

(F): Remit - The NIHR-BR supports several different programmes and each of these also have responsibility for their own Information Governance activities. Typically, this translates to the NIHR-BR having responsibility for centralised electronic records, and the separate studies and programmes have their own responsibility for the paper and / or electronic files at source.

(G): Responsibility and jurisdiction - Staff are employed by a number of organisations to provide this service. In many cases their parent legal entity and / or employment contract stipulates compliance and method of working. The policies described in this document are the master policies which pertain to this work but are supported by the institutional policies where applicable. Where these policies have a specific bearing on this work, they are explicitly referenced e.g. IG training. NIHR-BR, as a *grant*, cannot employ individuals. NIHR-BR staff are, in fact, employed by two separate departments of the University of Cambridge.

1 Management

1.1 Executive - Management Structure

1.1.1 The NIHR BioResource for translational research (NIHR-BR) is a grant, funded by the NIHR. It has an Oversight Board (which meets every six months), answerable to the UK Government's Department of Health and Social Care; a Steering Committee under that, comprised of scientific representatives of all the NIHR-funded regional BioResource Centres and initiatives, plus other major stakeholders; and under that an Operational Management Group (NIHR-BR OMG).

1.2 Executive - Management Commitment

1.2.1 The NIHR-BR Senior Management Team actively support information security within NIHR-BR through clear direction, demonstrated commitment, explicit assignment and acknowledgement of their, and everyone else's, information security responsibilities.

1.2.2 The NIHR-BR OMG has, in approving this Information Governance Policy, expressed clear support for information security and the management of identified information security risks that supports the business goals.

1.2.3 The NIHR-BR OMG have explicitly assigned lead responsibility for information security in the management team to the Information Governance Responsible Officer (IGRO)

1.2.4 The NIHR-BR OMG has allocated clear responsibilities to management and specific individuals for specific aspects of information security and these responsibilities are listed separately, in an IG Role Appointees document.

1.2.5 NIHR-BR OMG has ensured that there are adequate resources to provide the level of information security it requires.

1.2.6 NIHR-BR OMG, in acknowledging that it is not a legal entity, has sought and gained the oversight of the Information Governance team at Cambridge University Hospitals NHS Foundation Trust.

1.3 Executive - Security Policy

This policy specifies management's intent to protect electronic information assets within NIHR-BR from all threats, whether internal, external, deliberate or accidental. An information asset is (as defined by the UK National Archiving Government Body at www.nationalarchives.gov.uk), "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles."

An Information asset must be defined at a level of granularity that allows its constituent parts to be managed usefully as a single unit; too broad and you will not have enough detail, too fine and you will have thousands of assets.

1.3.1 This definition includes the following asset categories:

- Digital information assets in all formats including but not limited to; files, data, documents, reports, drawings, photographs, video, audio (including calls and recordings), intellectual property, licenses, and contracts
- Physical information assets including but not limited to physical documents; handwritten notes, drawings, and photographs.

1.3.2 Information within NIHR-BR exists in primarily electronic form and this policy intends to protect data stored electronically, transmitted across networks and less commonly on paper. The prime purpose of NIHR-BR's Information Governance policy is to protect and safeguard the information of the project, its service users and participants.

1.3.3 The objective of information security is to prevent and reduce the impact of security incidents. The implementation of this policy is mandatory to maintain and demonstrate the organisation's integrity in dealings with all our external parties.

1.3.4 NIHR-BR acknowledges that where its primary computing services are provided by an external third party, they are duly accredited and conform to best practice. Currently the organisation's environment is subject to access and management by a remote datacentre service provider (RDSP) which is AIMES Management Services Ltd. A service level agreement (SLA) must be signed by both parties, with information security being a critical part of the agreement.

1.3.5 It is the policy of NIHR-BR to ensure:

- Information is protected against unauthorised access
- Information is retained only for as long as it is required and has a relevant legal basis
- Information is preserved in line with our Systems Security Policy & Operational Security Policy
- Confidentiality of information is assured
- Information is not disclosed to unauthorised persons through deliberate or careless actions
- The integrity of information is maintained
- Information is available to authorised users when required
- Regulatory and legislative requirements are met
- Business continuity plans are produced, maintained and regularly tested
- Information security training is delivered to all staff
- All breaches of information security, actual and suspected are recorded, reported and investigated.

1.3.6 Standards, policies and security operating procedures that are available to support this policy include the University Acceptable Use Policy, Systems Security Policy, and Operational Security Policy. A formal disciplinary process operating through the employers of the individuals providing this service will be referenced and implemented for those employees who do not comply with standards, policies and procedures. Appropriate training is additionally provided to support staff to understand their obligations to comply with the above noted policies and procedures.

1.3.7 The IGRO, supported by the Information Governance Leads (IGLs), has overall responsibility for maintaining this policy and providing guidance on its implementation. All managers are responsible for implementing policies and procedures within their business areas. It is the responsibility of each employee to adhere to policies and procedures. Employees who do not adhere to the policies and procedures may be subject to disciplinary procedures.

1.3.8 This policy will be reviewed regularly, and at least biennially, to ensure it remains appropriate for NIHR-BR.

2 Key Principles

The security principles listed below have been selected to support staff in understanding their responsibilities for working securely with information and will help them in making security-conscious decisions in their day-to-day activities. These key Information Governance principles, and their associated lower-level guidelines and procedures, are written to ensure teams are working securely whilst maintaining standards in their ways of working with data.

Protecting Information

Our organisation is committed to maintaining the confidentiality, integrity and availability of information and associated systems. We are committed to ensuring we always employ mechanisms for data protection, and governance when working with our data.

All staff must equally appreciate their unique responsibilities for working to maintain the confidentiality, integrity, privacy, quality and availability of data by applying the principles in this policy and those outlined in the associated procedures and standards.

Data Protection and GDPR

Our organisation maintains adherence to all applicable data protection legislation, including, where applicable the UK General Data Protection Regulation and Data Protection Act 2018.

We strive to ensure that we incorporate the below listed principles in our ways of working with data:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Information Classification

Information is classified in a manner that ensures its security and maintains its integrity.

Information owners are responsible for assigning classifications to information assets according to the information classification standard.

Information Handling

Correct handling of confidential and personal data is vital to the services that the NIHR BioResource provides. Therefore it is crucial for staff to follow the defined Information Governance and Security Procedures. All staff must adhere to the appropriate information handling procedures when on and offsite. Access to the organisation's information assets and associated processing systems, and especially personal information, will be restricted consistently with the information handling guidelines and procedures.

All members of staff are expected to store any sensitive information in a secure location. Information assets must not be left exposed or in open view.

The organisation ensures procedures and systems are in place to implement appropriate access controls, to ensure that information is stored and transported securely and is not lost or corrupted.

Our physical data is of equal importance. We are a clear desk organisation and data is only ever printed and/or maintained in a physical format where absolutely necessary. Approved destruction methods are adopted upon termination of use.

Acceptable Use of Assets

All usage of NIHR-BioResource assets must be reasonable, appropriate, and not impact upon the performance of normal business or duties.

Staff must ensure they read and understand the parent organisation's (University of Cambridge) Acceptable Use Policy. Staff accessing the organisation's data, whether on an organisationally provisioned device or not, will have their access monitored and if necessary, restricted.

Staff must follow the organisation's Incident Reporting Procedure to ensure any data security or governance related issues with their provisioned device is reported through the appropriate mechanisms.

User Access Management

The organisation ensures that no individual is allocated responsibility for or given access to more parts of the system(s) than is necessary to perform their duties.

Where practicable, NIHR-BR's operations will be structured with roles and responsibilities allocated to avoid overlapping areas of interest. Where this is not possible supervision and shared controls will be used to minimise threats, which may arise from such overlaps.

Users – Terms and Conditions

Before gaining access to the NIHR-BR's secure systems, all visitors and external staff/partners must have agreed to a confidentiality and access agreement between their employer or agent and the University of Cambridge or Cambridge University Hospitals NHS Foundation Trust.

Users shall not at any time during access to the NIHR-BR's secure systems, or at any time afterwards, disclose to any person any information that would compromise the privacy of any individual participants, compromise the practical business dealings or affairs of NIHR-BR or as to any other matters which may come to their knowledge by reason of their access.

Users – Teleworking

Teleworking is defined as working at home or at any other private off-site locations that are linked electronically to a central office or principal place of employment. Teleworking is a cooperative arrangement between NIHR-BR and its employees, contractors, and associated personnel.

NIHR-BR is committed to develop, maintain and support a comprehensive policy of equal opportunities in employment within NIHR-BR. To assist in this, and in line with University policy, NIHR-BR will actively support teleworking where it is reasonable and practical to do so and where operational needs would not be adversely affected.

	Where staff are working offsite or teleworking, they are expected to adhere to the Teleworking policy requirements (found in the Acceptable Use Policy) and ensure they adhere to the guidelines of Teleworking published in the Acceptable Use Policy.
Personally Identifiable Information (PID)	Other than to contact the participant themselves, Personal Identifiable Data (PID) can only be sent over secure communications channels that have been approved and tested by the NIHR-BR Information Security / Information Technology team, or are otherwise accredited by NHS Digital e.g. NHS Mail.
Defence in Depth	The NIHR-BR will seek to ensure that Security mechanisms are layered in such a manner that the weaknesses of one mechanism are countered by the strengths of one or more other different mechanisms. This helps to provide resilience against different forms of attack and reduces the probability of a single point of failure or compromise.
Assign least privilege	Environments, systems and applications are configured to provide no more authorisation to any individual user account than is necessary to perform required functions. Consideration is given to implementing role-based access controls (RBAC) for various aspects of system use, not only administration.
Incident Management	The NIHR-BR ensures a rapid response to incidents that threaten the Confidentiality, Integrity, and Availability (CIA) of NIHR-BR's information assets, information systems, and require all staff to be understand their responsibilities for helping to prevent incidents or reduce their impact. Where security incidents arise through accidental, intentional misuse or negligence, a security incident issue shall be completed in the Incident Log once the incident has been identified. The competence of the individual(s) responsible and processes that they were following, shall be re-assessed. Training and process re-engineering will be discussed if the incident is found to be accidental or unintentional and / or repeated.
Design for Updating	Security is designed to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
Physical Security	To ensure a high degree of information protection, physical security is a critical part in keeping a high and effective information security posture. It is critical that only authorized persons have access to the NIHR BioResource premises. NIHR BioResource maintains a clear-desk policy to further enhance the physical security controls implemented within working areas.
Interoperability	Where possible, security of systems and applications are based on open standards for portability and interoperability. For security capabilities to be effective, the team makes every effort to incorporate interoperability and portability into all security measures, including hardware and software, and implementation practices.

Separation of Duties	The Organisation ensures the clear separation of tasks and functions between different roles to provide a layer of accountability and protection.
Secure Defaults	Every application, service and process is implemented securely by default. Administrators decide to reduce security only by exception and if the application and / or business process requires it, but default configuration settings should be the most secure possible.
Training and Awareness	NIHR-BR implements a programme for providing appropriate information security awareness and training to all users / staff. Our Training Needs Analysis will address any gaps in skillset to ensure training is targeted where relevant.
Privacy by Design	The organisation always ensures that the introduction of any new systems or processes that involve personal data use is undertaken with the aim to protect personal information of individuals and ensure the application of privacy related regulations that are relevant to the organisational environment.
Security Culture	The organisation ensures that all staff are trained in and understand their individual role in achieving a sound security culture.
Zero Trust (Identity-Driven Access Control)	The NIHR BR is adopting the principle of Zero Trust, which is based on the concept that network perimeters or boundaries are no longer clearly defined in governing access to data or other resources. Instead, trust (access) is granted to specific individuals in specific contexts for specific purposes. Trust is not assumed, but rather only granted when the individual has demonstrated that they are who they say they are and have the appropriate authority.
Auditing and Monitoring	The organisation ensures that Internal audits or spot checks are conducted on-site at least once a year, in line with regulatory expectations.

3 Who Must Follow This Policy?

This policy is mandatory for all staff working within the NIHR BioResource organisation. The NIHR BioResource is also committed to having its third-party partners and vendors meet the requirements set out herein. Depending on the seriousness, failure to comply with our policies may lead to disciplinary action.

Staff that choose not to follow the specified requirements contained within the security procedures and policies of the organisation shall be subject to the disciplinary process of the relevant organisation.

4 Questions and Support

For specific questions and or feedback on this policy, please contact:

- **The NIHR BioResource Information Governance & Information Security team**
  Email: ig@bioresource.nihr.ac.uk

- **The Data Protection Officer**

Michelle Ellerbeck
Information governance lead/Data Protection Officer
Cambridge University Hospitals NHS Foundation Trust
Box 153
Hills Road
Cambridge
CB2 0QQ

Email gdpr.enquiries@addenbrookes.nhs.uk

5 Further Links

5.1.1 The NIHR BioResource organisation in acknowledging that it is not a legal entity, has sought and gained the oversight of the Information Governance team at Cambridge University Hospitals NHS Foundation Trust and University of Cambridge. Our Information Governance Policy is therefore to be followed in conjunction with the below associated policies to ensure a comprehensive understanding of all the obligations on the staff members of our organisation and consequently the University of Cambridge.

a. **University of Cambridge, School of Clinical Medicine – Acceptable Use Policy**

https://cscs.medschl.cam.ac.uk/about-us/policies/cscs-aup/

b. **University of Cambridge, School of Clinical Medicine – Information Security Policy**

https://www.medschl.cam.ac.uk/about/computing/information-security-policy/

c. **Cambridge University Hospitals NHS Foundation Trust - Information governance and information security policy**
https://www.cuh.nhs.uk/documents/51/Information_governance_and_information_security_policy_Version13.1_2.pdf